

This listing of claims will replace all prior versions, and listings, of claims in the application.

**Listing of Claims:**

1. (currently amended) A computer-implemented method for controlling ~~controlling~~ access to documents during a workflow, comprising:

upon entry of a base document into a workflow, creating a working copy of the base document;

selectively providing a user access to ~~either the base document or the working copy of the base document~~ depending upon the identity of a user;

selectively providing a user access to the working copy of the base document depending upon the identity of a user; and

if a user is provided access to the working copy of the base document, selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user.

2. (original) The method of claim 1, further comprising:

storing access control list data in relation to the base document, the access control list data defining access controls on performing operations of the working copy of the base document; and

storing security descriptor data in relation to the base document and the working copy of the base document, the security descriptor data defining access controls on reading the base document and the working copy of the base document.

3. (currently amended) The method of claim 2, wherein ~~the step of~~ selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, ~~further~~ comprises:

determining using the access control list data stored in relation to the base document that a user has permission to perform an operation on the copy of the base document; and  
allowing the user to perform the operation on the copy of the base document.

4. (currently amended) The method of claim 2, wherein the step of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, ~~further~~ comprises:

B  
1  
determining using the access control list data stored in relation to the base document that a user does not have permission to perform an operation on the copy of the base document; and  
denying the user access to perform the operation on the copy of the base document.

5. (currently amended) The method of claim 2, wherein the access control list data comprises information identifying for each of a plurality of operations, the set of users that have permission to perform the operation, and said act of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, ~~further~~ comprises:

referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation; and

if the user is in the set of users that have permission to perform the operation, providing access to the operation.

6. (currently amended) The method of claim 2, wherein the access control list data comprises information identifying for each of a plurality of operations, the set of users that have permission to perform the operation, and said act of selectively providing access to perform operations on the working copy of the base document depending upon the identity of a user, ~~further~~ comprises:

referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation; and

-----if the user is not in the set of users that have permission to perform the operation,  
denying access to the operation.

7. (currently amended) The method of claim 5, wherein the set of users are defined in terms of the roles that have permission to perform the operation, and said act of referencing the information identifying for each of a plurality of operations, the set of users that have permission to perform the operation, further comprises:

resolving for the user the set of roles to which the user has been assigned; and  
determining using the set of roles to which the user has been assigned and the set of users defined in terms of the roles that have permission to perform the operation, whether the user has permission to perform the requested operation.

8. (currently amended) The method of claim 2, wherein ~~the step of~~ selectively providing a user access to ~~either the base document or the working copy of the base document~~ depending upon the identity of a user, further comprises:

determining using the security descriptor data stored in relation to the base document and the working copy document, that a user has permission to read the working copy of the base document; and

providing the user access to the working copy of the base document.

9. (currently amended) The method of claim 2, wherein ~~the step of~~ selectively providing a user access to ~~either the base document or the working copy of the base document~~ depending upon the identity of a user, further comprises:

determining using the security descriptor data stored in relation to the base document and the working copy document, that a user does not have permission to read the working copy of the base document; and

denying the user access to the working copy of the base document.

10. (currently amended) - The method of claim 2, wherein the security descriptor data comprises information identifying the set of users that have permission to read each of the base document and the working copy of the base document, and said act of selectively providing access to ~~either the base document or the working copy of the base document~~ documents depending on the identity of the user, ~~further~~ comprises:

referencing the information identifying the set of users that have permission to read each of the base document and the working copy of the base document; and

if the user is in the set of users that have permission to read the working copy of the base document, providing access to the working copy of the base document.

11. (currently amended) The method of claim 10, wherein the set of users are defined in terms of the roles that have permission to read each of the base document and the working copy of the base document, and said act of referencing the information identifying the set of users that have permission to read each of the base document and the working copy of the base document, ~~further~~ comprises:

resolving for the user the set of roles to which the user has been assigned; and

determining using the set of roles to which the user has been assigned and the set of ~~user-defined in terms of the~~ roles that have permission to read each of the base document and the working copy of the base document, whether the user has permission to read the base document or the working copy of the base document.

12. (original) A computer-readable media having stored thereon computer-executable instructions for performing the steps recited in claim 1.

13. (currently amended) A system for providing document isolation in a workflow environment, comprising:

a processor, wherein said processor is operable to execute instructions for performing the following acts:

maintaining for a base document undergoing a publishing workflow, a copy of the base document;

maintaining access control data in relation to the base document and the copy of the base document; ~~and~~

upon receipt of a request to access the base document, selectively determining based on the access control data to provide access to ~~either the base document or the copy of the base document~~; and

upon receipt of a request to access the base document, selectively determining based on the access control data to provide access to the copy of the base document.

14. (original) The system of claim 13, wherein the access control data comprises security descriptor data identifying the set of users that have permission to read the base document and the copy of the base document.

15. (currently amended) The system of claim 14, wherein said processor is operable to execute instructions for performing the following ~~further~~ acts:

referencing the security descriptor data; and

determining that a user should be directed to the copy of the base document based on the security descriptor data.

16. (currently amended) The system of claim 15, wherein the security descriptor data identifies a set of roles corresponding to the set of users that have permission to read the base document and the copy of the base document, and wherein said processor is operable to execute instructions for performing the ~~further~~ act of determining the set of roles that a user has been assigned.

17. (original) The system of claim 13, wherein the access control data comprises access control list data identifying the set of users that have permission to perform operations on the copy of the base document.

18. (currently amended) The system of claim 17, wherein said processor is operable to execute instructions for performing the following ~~further~~ acts:

referencing the access control list data; and

determining that a user should be allowed to perform an operation on the copy of the base document based on the access control list data.

19. (currently amended) The system of claim 18, wherein the access control list data identifies a set of roles corresponding to the set of users that have permission to perform operations on the copy of the base document, and wherein said processor is operable to execute instructions for performing the ~~further~~ act of determining the set of roles that a user has been assigned.

20. (currently amended) A method for controlling access to operations that may be performed on a document, of updating access controls to reflect the addition of a new operation that may be performed on a copy of a base document, in a system wherein access to operations to be performed on a copy of the base document are controlled using an access control list which identifies the operations that may be performed and the roles that a user must have to access these operations, comprising:

upon creation of a workflow, creating a copy of a base document;

receiving a request to create a new operation that may be performed on the copy of the base document;

assigning a unique identifier to the new operation that may be performed on a copy of a base document;

updating an the access control list to include an entry for the unique identifier for the new operation; and

updating the access control list to include an entry identifying the roles that have access to the new operation.

21. (new) The method of claim 20, further comprising updating the access control list to change roles that have access to the new operation in response to a change in the state occupied by the working copy of the document in the workflow.

22. (new) The method of claim 20, wherein the workflow is a publishing workflow and the new operation is at least one of the following: review and approve.

23. (new) The method of claim 20, further comprising:  
receiving a request to perform the new operation on the copy of the base document;  
determining using the access control list whether to allow access to the new operation.

24. (new) The method of claim 23, wherein determining using the access control list whether to allow access to the new operation comprises comparing a user's roles with the roles identified in the access control list as having access to the new operation.

25. (new) A computer-implemented method of controlling access to documents, comprising:  
maintaining a first list defining who may access a base document;  
maintaining a second list defining who may perform operations on the base document;  
upon receipt of a request from a user to create a workflow, accessing the first list and the second list to determine whether the user may create a workflow relating to the base document;  
if the first list and the second list indicate the user may create a workflow relating to the base document, creating a copy of the base document; and

while the copy of the base document is in the workflow, in response to requests to access the base document, accessing at least the first list to determine whether to provide access to the copy of the base document.

26. (new) The method of claim 25, wherein maintaining a first list defining who may access a base document comprises maintaining a list of security descriptors.

27. (new) The method of claim 25, wherein maintaining a second list defining who may perform operations on the base document comprises maintaining an access control list.

28. (new) The method of claim 25, further comprising updating the second list upon creation of the copy of the base document to identify who may perform operations on the copy of the base document.

29. (new) The method of claim 25, wherein maintaining a first list defining who may access a base document comprises maintaining a first list defining roles that may access a base document.

30. (new) The method of claim 25, further comprising maintaining a third list defining who may access the copy of the base document.